

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-126915

(43)Date of publication of application : 22.04.2004

(51)Int.Cl. G06F 7/58
G09C 1/00
H03K 3/84

(21)Application number : 2002-289825

(71)Applicant : COMMUNICATION RESEARCH
LABORATORY

(22)Date of filing : 02.10.2002

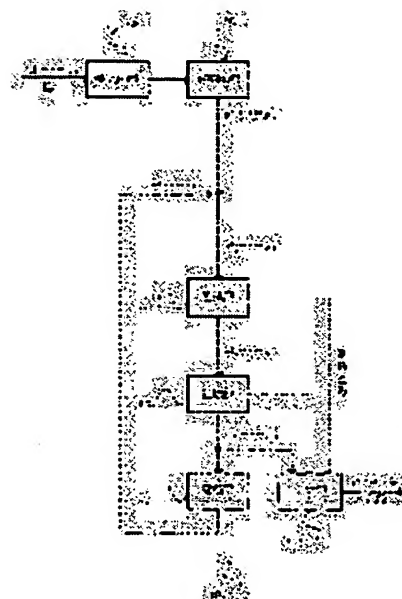
(72)Inventor : UMEMO TAKESHI

(54) RANDOM NUMBER SEQUENCE GENERATION DEVICE, RANDOM NUMBER SEQUENCE GENERATION METHOD, AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a random number sequence generation device by which a generated random number sequence has favorable natures as the random number sequence, and to provide a random number sequence generation method, and a program for materializing the device and the method by means of a computer.

SOLUTION: The pilot reception section 102 of the random number sequence generation device 101 receives the integer string of w bits as a pilot. An initialization section 103 provides the integer string of the received pilot to a conversion section 104. The conversion section 104 applies conversion defined by nonlinear conversion g to the respective provided integer strings to obtain the integer string of the w bits. A rotation section 105 conducts the specified rotation operation by understanding the obtained integer string as the bit string of wn bits to obtain the integer string of the w bits from the obtained bit string of the wn bits. An output section 107 determines that whether or not conversion in the conversion section 104 and rotation in the rotation section 105 are repeated by the specified number of times, and finally, outputs the integer string obtained from the rotation section 105 as the random number sequence. A renewal section 106 provides the integer string obtained from the rotation section 105 to the conversion section 104 to repeat processing.



LEGAL STATUS

[Date of request for examination]

02.10.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-126915

(P2004-126915A)

(43) 公開日 平成16年4月22日(2004. 4. 22)

(51) Int. Cl.⁷

F I

テーマコード (参考)

G06F 7/58

G06F 7/58

B

5J049

G09C 1/00

G09C 1/00

650B

5J104

H03K 3/84

H03K 3/84

Z

審査請求 有 請求項の数 26 O L (全 15 頁)

(21) 出願番号

特願2002-289825 (P2002-289825)

(22) 出願日

平成14年10月2日(2002. 10. 2)

(71) 出願人 301022471

独立行政法人通信総合研究所

東京都小金井市貫井北町4-2-1

(74) 代理人 100095407

弁理士 木村 潤

(74) 代理人 100110135

弁理士 石井 裕一郎

(72) 発明者 梅野 健

東京都小金井市貫井北町4-2-1 独立

行政法人通信総合研究所内

Fターム(参考) 5J049 AA00 AA31 CA05

5J104 AA18 FA05 NA04 NA09 NA10
NA17

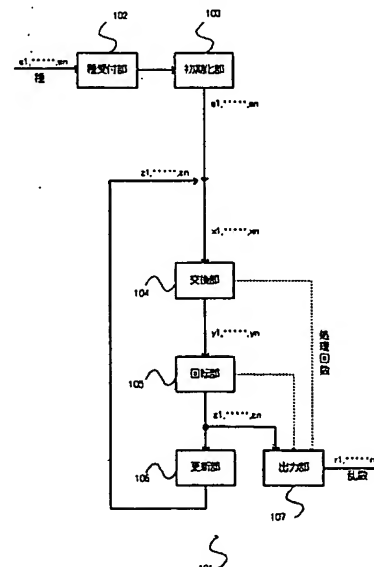
(54) 【発明の名称】 乱数列生成装置、乱数列生成方法、ならびに、プログラム

(57) 【要約】

【課題】 乱数列生成装置等を提供する。

【解決手段】 乱数列生成装置101の種受付部102は、wビットの整数の列を種として受け付け、初期化部103は、当該受け付けられた種の整数列を変換部104に与え、変換部104は、当該与えられた整数列のそれぞれに対して非線型変換 $g(\cdot, \cdot)$ により定義される変換を施してwビットの整数の列を得て、回転部105は、当該得られた整数の列をwnビットのビット列と見て所定の回転演算を行って、得られたwnビットのビット列からwビットの整数の列を得て、出力部107は、変換部104における変換ならびに回転部105における回転が、所定の回数繰り返されたか否かを判定し、最後に回転部105により得られた整数の列を、乱数列として出力し、更新部106は、当該回転部105により得られた整数の列を変換部104に与えて、処理を繰り返す。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

w ビットの乱数の列を生成する乱数列生成装置であって、種受付部と、初期化部と、変換部と、回転部と、更新部と、出力部と、を備え、

前記種受付部は、w ビットの整数の列 s_1, s_2, \dots, s_n を種として受け付け、

前記初期化部は、当該受け付けられた整数の列 s_1, s_2, \dots, s_n を、整数列 x_1, x_2, \dots, x_n として前記変換部に与え、

前記変換部は、当該与えられた整数列 x_1, x_2, \dots, x_n のそれぞれに対して所定の変換を施して w ビットの整数の列 y_1, y_2, \dots, y_n を得て、

前記回転部は、当該整数の列 y_1, y_2, \dots, y_n を wn ビットのビット列と見て所定の回転演算を行って、得られた wn ビットのビット列から w ビットの整数の列 z_1, z_2, \dots, z_n を得て、

前記更新部は、当該整数の列 z_1, z_2, \dots, z_n を整数列 x_1, x_2, \dots, x_n として前記変換部に与え、

前記出力部は、前記変換部における変換ならびに前記回転部における回転が、所定の回数繰り返された場合、最後に得られた z_1, z_2, \dots, z_n を、乱数列 r_1, r_2, \dots, r_n として出力する

ことを特徴とするもの。

【請求項 2】

請求項 1 に記載の乱数列生成装置であって、

前記変換部は、写像 $g(\cdot, \cdot)$ を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_1 = g(x_n, x_1);$$

$$y_{i+1} = g(x_i, x_{i+1})$$

により変換を行う

ことを特徴とするもの。

【請求項 3】

請求項 1 に記載の乱数列生成装置であって、

前記変換部は、所定の整数 c と、写像 $g(\cdot, \cdot)$ と、を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_1 = g(c, x_1);$$

$$y_{i+1} = g(y_i, x_{i+1})$$

により変換を行う

ことを特徴とするもの。

【請求項 4】

請求項 1 に記載の乱数列生成装置であって、

前記変換部は、写像 $g(\cdot, \cdot)$ を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_1 = g(c, x_1);$$

$$y_{i+1} = g(x_i, x_{i+1})$$

により変換を行う

ことを特徴とするもの。

【請求項 5】

請求項 2 から 4 のいずれか 1 項に記載の乱数列生成装置であって、

当該写像 $g(\cdot, \cdot)$ は、所定の写像 $h(\cdot)$ と所定の整数 q ($0 \leq q \leq 2^w - 1$) により

$$g(a, b) = 2b^2 + h(a)b + q \pmod{2^w}$$

と定義される

ことを特徴とするもの。

【請求項 6】

10

20

30

40

50

請求項 5 に記載の乱数列生成装置であって、当該写像 $h(\cdot)$ は、

$$h(a) = a$$

と定義される

ことを特徴とするもの。

【請求項 7】

請求項 5 に記載の乱数列生成装置であって、

当該写像 $h(\cdot)$ は、与えられた値の数値表現の所定のビットをクリアする演算により定義される

ことを特徴とするもの。

【請求項 8】

請求項 5 に記載の乱数列生成装置であって、

当該写像 $h(\cdot)$ は、与えられた値の数値表現の所定のビットを反転する演算により定義される

ことを特徴とするもの。

【請求項 9】

請求項 5 に記載の乱数列生成装置であって、

当該写像 $h(\cdot)$ は、与えられた値の数値表現の最下位 2 ビットを 0 1 に置換する演算により定義される

ことを特徴とするもの。

【請求項 10】

請求項 1 から 9 のいずれか 1 項に記載の乱数列生成装置であって、

前記回転部は、当該所定の回転演算として、当該 wn ビットのビット列を所定のビット数だけ巡回シフトする

ことを特徴とするもの。

【請求項 11】

請求項 1 から 9 のいずれか 1 項に記載の乱数列生成装置であって、

前記回転部は、他の乱数をさらに取得し、当該所定の回転演算は、当該整数列 y_1, y_2, \dots, y_n を回転させる回転方向および回転ビット数は、当該他の乱数の値によって決まる

ことを特徴とするもの。

【請求項 12】

請求項 1 から 9 のいずれか 1 項に記載の乱数列生成装置であって、

前記回転部は、他の乱数をさらに取得し、当該所定の回転演算は、当該他の乱数が所定の値である場合、当該整数列 y_1, y_2, \dots, y_n を所定のビット数だけある方向に回転し、そうでない場合、これとは逆の方向に回転する

ことを特徴とするもの。

【請求項 13】

w ビットの乱数の列を生成する乱数列生成方法であって、種受付工程と、初期化工程と、変換工程と、回転工程と、更新工程と、出力工程と、を備え、

前記種受付工程では、 w ビットの整数の列 s_1, s_2, \dots, s_n を種として受け付け、前記初期化工程では、当該受け付けられた整数の列 s_1, s_2, \dots, s_n を、整数列 x_1, x_2, \dots, x_n として前記変換工程に与え、

前記変換工程では、当該与えられた整数列 x_1, x_2, \dots, x_n のそれぞれに対して所定の変換を施して w ビットの整数の列 y_1, y_2, \dots, y_n を得て、

前記回転工程では、当該整数の列 y_1, y_2, \dots, y_n を wn ビットのビット列と見て所定の回転演算を行って、得られた wn ビットのビット列から w ビットの整数の列 z_1, z_2, \dots, z_n を得て、

前記更新工程では、当該整数の列 z_1, z_2, \dots, z_n を整数列 x_1, x_2, \dots, x_n として前記変換工程に与え、

前記出力工程では、前記変換工程における変換ならびに前記回転工程における回転が、所

10

20

30

40

50

定の回数繰り返された場合、最後に得られた整数の列 z_1, z_2, \dots, z_n を、乱数列 r_1, r_2, \dots, r_n として出力することを特徴とする方法。

【請求項 14】

請求項 13 に記載の乱数列生成方法であって、前記変換工程では、写像 $g(\cdot, \cdot)$ を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_1 = g(x_n, x_1);$$

$$y_{i+1} = g(x_i, x_{i+1})$$

により変換を行う

ことを特徴とする方法。

10

【請求項 15】

請求項 13 に記載の乱数列生成方法であって、前記変換工程では、所定の整数 c と、写像 $g(\cdot, \cdot)$ と、を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_1 = g(c, x_1);$$

$$y_{i+1} = g(y_i, x_{i+1})$$

により変換を行う

ことを特徴とする方法。

20

【請求項 16】

請求項 13 に記載の乱数列生成方法であって、前記変換工程では、写像 $g(\cdot, \cdot)$ を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_1 = g(c, x_1);$$

$$y_{i+1} = g(x_i, x_{i+1})$$

により変換を行う

ことを特徴とする方法。

【請求項 17】

請求項 14 から 16 のいずれか 1 項に記載の乱数列生成方法であって、当該写像 $g(\cdot, \cdot)$ は、所定の写像 $h(\cdot)$ と所定の整数 q ($0 \leq q \leq 2^w - 1$) により

$$g(a, b) = 2b^2 + h(a)b + q \pmod{2^w}$$

と定義される

ことを特徴とする方法。

30

【請求項 18】

請求項 17 に記載の乱数列生成方法であって、当該写像 $h(\cdot)$ は、

$$h(a) = a$$

と定義される

ことを特徴とする方法。

【請求項 19】

請求項 17 に記載の乱数列生成方法であって、

当該写像 $h(\cdot)$ は、与えられた値の数値表現の所定のビットをクリアする演算により定義される

ことを特徴とする方法。

40

【請求項 20】

請求項 17 に記載の乱数列生成方法であって、

当該写像 $h(\cdot)$ は、与えられた値の数値表現の所定のビットを反転する演算により定義される

ことを特徴とする方法。

【請求項 21】

50

請求項 1 7 に記載の乱数列生成方法であって、
当該写像 $h(\cdot)$ は、与えられた値の数値表現の最下位 2 ビットを 0 1 に置換する演算により定義される
ことを特徴とする方法。

【請求項 2 2】

請求項 1 3 から 2 1 のいずれか 1 項に記載の乱数列生成方法であって、
前記回転工程では、当該所定の回転演算として、当該 w_n ビットのビット列を所定のビット数だけ巡回シフトする
ことを特徴とする方法。

【請求項 2 3】

請求項 1 3 から 2 1 のいずれか 1 項に記載の乱数列生成方法であって、
前記回転工程では、他の乱数をさらに取得し、当該所定の回転演算は、当該整数列 y_1, y_2, \dots, y_n を回転させる回転方向および回転ビット数は、当該他の乱数の値によって決まる
ことを特徴とする方法。

【請求項 2 4】

請求項 1 3 から 2 1 のいずれか 1 項に記載の乱数列生成方法であって、
前記回転工程では、他の乱数をさらに取得し、当該所定の回転演算は、当該他の乱数が所定の値である場合、当該整数列 y_1, y_2, \dots, y_n を所定のビット数だけある方向に回転し、そうでない場合、これとは逆の方向に回転する
ことを特徴とする方法。

【請求項 2 5】

コンピュータを、請求項 1 から 1 2 のいずれか 1 項に記載の乱数列生成装置として機能させることを特徴とするプログラム。

【請求項 2 6】

コンピュータに、請求項 1 3 から 2 4 のいずれか 1 項に記載の乱数列生成方法を実行させることを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、乱数列生成装置、乱数列生成方法、ならびに、プログラムに関する。

【0002】

【従来の技術】

従来から、種々の乱数列生成のための技術が提案されている。これらの技術によって得られた乱数は、たとえば、モンテカルロ法による各種の物理現象、化学現象などの模擬実験や、秘密通信のブロック暗号システムにおいて用いられる。

【0003】

【発明が解決しようとする課題】

さて、このような乱数列の生成技術においては、得られた乱数列に含まれる数値の分布ができるだけ一様であることや、当該数値のコンピュータにおける数値表現の所定のビットのみを見た場合に、当該ビットの「0」と「1」の出現頻度にできるだけ偏りがいないことや、乱数列の周期ができるだけ長いことなど、種々の性質を満たすことが望ましい。

【0004】

本発明は、生成される乱数列が乱数列として好ましい性質を有するような乱数列生成装置、乱数列生成方法、ならびに、これらをコンピュータによって実現するためのプログラムを提供することを目的とする。

【0005】

【課題を解決するための手段】

以上の目的を達成するため、本発明の原理にしたがって、下記の発明を開示する。

【0006】

10

20

30

40

50

本発明の第1の観点に係る乱数生成装置は、wビットの乱数の列を生成し、種受付部と、初期化部と、変換部と、回転部と、更新部と、出力部と、を備え、以下のように構成する。

【0007】

すなわち、種受付部は、wビットの整数の列 s_1, s_2, \dots, s_n を種として受け付ける。

【0008】

一方、初期化部は、当該受け付けられた整数の列 s_1, s_2, \dots, s_n を、整数列 x_1, x_2, \dots, x_n として変換部に与える。

【0009】

さらに、変換部は、当該与えられた整数列 x_1, x_2, \dots, x_n のそれぞれに対して所定の変換を施してwビットの整数の列 y_1, y_2, \dots, y_n を得る。

【0010】

そして、回転部は、当該整数の列 y_1, y_2, \dots, y_n をwnビットのビット列と見て所定の回転演算を行って、得られたwnビットのビット列からwビットの整数の列 z_1, z_2, \dots, z_n を得る。

【0011】

一方、更新部は、当該整数の列 z_1, z_2, \dots, z_n を整数列 x_1, x_2, \dots, x_n として変換部に与える。

【0012】

さらに、出力部は、変換部における変換ならびに回転部における回転が、所定の回数繰り返された場合、最後に得られた整数の列 z_1, z_2, \dots, z_n を、乱数列 r_1, r_2, \dots, r_n として出力する。

【0013】

また、本発明の乱数列生成装置において、変換部は、写像 $g(\cdot, \cdot)$ を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_1 = g(x_n, x_1);$$

$$y_{i+1} = g(x_i, x_{i+1})$$

により変換を行うように構成することができる。

【0014】

また、本発明の乱数列生成装置において、変換部は、所定の整数 c と、写像 $g(\cdot, \cdot)$ と、を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_1 = g(c, x_1);$$

$$y_{i+1} = g(y_i, x_{i+1})$$

により変換を行うように構成することができる。

【0015】

また、本発明の乱数列生成装置において、変換部は、写像 $g(\cdot, \cdot)$ を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_1 = g(c, x_1);$$

$$y_{i+1} = g(x_i, x_{i+1})$$

により変換を行うように構成することができる。

【0016】

また、本発明の乱数列生成装置において、当該写像 $g(\cdot, \cdot)$ は、所定の写像 $h(\cdot)$ と所定の整数 q ($0 \leq q \leq 2^w - 1$) により

$$g(a, b) = 2b^2 + h(a)b + q \pmod{2^w}$$

と定義されるように構成することができる。

【0017】

また、本発明の乱数列生成装置において、当該写像 $h(\cdot)$ は、

$$h(a) = a$$

と定義されるように構成することができる。

10

20

30

40

50

【0018】

また、本発明の乱数列生成装置において、当該写像 $h(\cdot)$ は、与えられた値の数値表現の所定のビットをクリアする演算により定義されるように構成することができる。

【0019】

また、本発明の乱数列生成装置において、当該写像 $h(\cdot)$ は、与えられた値の数値表現の所定のビットを反転する演算により定義されるように構成することができる。

【0020】

また、本発明の乱数列生成装置において、当該写像 $h(\cdot)$ は、与えられた値の数値表現の最下位2ビットを01に置換する演算により定義されるように構成することができる。

【0021】

また、本発明の乱数列生成装置において、回転部は、当該所定の回転演算として、当該 w ビットのビット列を所定のビット数だけ巡回シフトするように構成することができる。

【0022】

また、本発明の乱数列生成装置において、回転部は、他の乱数をさらに取得し、当該所定の回転演算は、当該整数列 y_1, y_2, \dots, y_n を回転させる回転方向および回転ビット数は、当該他の乱数の値によって決まるように構成することができる。

【0023】

また、本発明の乱数列生成装置において、回転部は、他の乱数をさらに取得し、当該所定の回転演算は、当該他の乱数が所定の値である場合、当該整数列 y_1, y_2, \dots, y_n を所定のビット数だけある方向に回転し、そうでない場合、これとは逆の方向に回転するように構成することができる。

【0024】

本発明の他の観点に係る乱数列生成方法は、 w ビットの乱数の列を生成し、種受付工程と、初期化工程と、変換工程と、回転工程と、更新工程と、出力工程と、を備え、以下のよう構成する。

【0025】

すなわち、種受付工程では、 w ビットの整数の列 s_1, s_2, \dots, s_n を種として受け付ける。

【0026】

一方、初期化工程では、当該受け付けられた整数の列 s_1, s_2, \dots, s_n を、整数列 x_1, x_2, \dots, x_n として変換工程に与える。

【0027】

さらに、変換工程では、当該与えられた整数列 x_1, x_2, \dots, x_n のそれぞれに対して所定の変換を施して w ビットの整数の列 y_1, y_2, \dots, y_n を得る。

【0028】

そして、回転工程では、当該整数の列 y_1, y_2, \dots, y_n を w ビットのビット列と見て所定の回転演算を行って、得られた w ビットのビット列から w ビットの整数の列 z_1, z_2, \dots, z_n を得る。

【0029】

一方、更新工程では、当該整数の列 z_1, z_2, \dots, z_n を整数列 x_1, x_2, \dots, x_n として変換工程に与える。

【0030】

さらに、出力工程では、変換工程における変換ならびに回転工程における回転が、所定の回数繰り返された場合、最後に得られた整数の列 z_1, z_2, \dots, z_n を、乱数列 r_1, r_2, \dots, r_n として出力する。

【0031】

また、本発明の乱数列生成方法において、変換工程では、写像 $g(\cdot, \cdot)$ を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$\begin{aligned} y_i &= g(x_n, x_1); \\ y_{i+1} &= g(x_i, x_{i+1}) \end{aligned}$$

10

20

30

40

50

により変換を行うように構成することができる。

【0032】

また、本発明の乱数列生成方法において、変換工程では、所定の整数 c と、写像 $g(\cdot, \cdot)$ と、を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_1 = g(c, x_1);$$

$$y_{i+1} = g(y_i, x_{i+1})$$

により変換を行うように構成することができる。

【0033】

また、本発明の乱数列生成方法において、変換工程では、写像 $g(\cdot, \cdot)$ を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_1 = g(c, x_1);$$

$$y_{i+1} = g(x_i, x_{i+1})$$

により変換を行うように構成することができる。

【0034】

また、本発明の乱数列生成方法において、当該写像 $g(\cdot, \cdot)$ は、所定の写像 $h(\cdot)$ と所定の整数 q ($0 \leq q \leq 2^w - 1$) により

$$g(a, b) = 2b^2 + h(a)b + q \pmod{2^w}$$

と定義されるように構成することができる。

【0035】

また、本発明の乱数列生成方法において、当該写像 $h(\cdot)$ は、

$$h(a) = a$$

と定義されるように構成することができる。

【0036】

また、本発明の乱数列生成方法であって、当該写像 $h(\cdot)$ は、与えられた値の数値表現の所定のビットをクリアする演算により定義されるように構成することができる。

【0037】

また、本発明の乱数列生成方法において、当該写像 $h(\cdot)$ は、与えられた値の数値表現の所定のビットを反転する演算により定義されるように構成することができる。

【0038】

また、本発明の乱数列生成方法において、当該写像 $h(\cdot)$ は、与えられた値の数値表現の最下位2ビットを01に置換する演算により定義されるように構成することができる。

【0039】

また、本発明の乱数列生成方法において、回転工程では、当該所定の回転演算として、当該 wn ビットのビット列を所定のビット数だけ巡回シフトするように構成することができる。

【0040】

また、本発明の乱数列生成方法において、回転工程では、他の乱数をさらに取得し、当該所定の回転演算は、当該整数列 y_1, y_2, \dots, y_n を回転させる回転方向および回転ビット数は、当該他の乱数の値によって決まるように構成することができる。

【0041】

また、本発明の乱数列生成方法において、回転工程では、他の乱数をさらに取得し、当該所定の回転演算は、当該他の乱数が所定の値である場合、当該整数列 y_1, y_2, \dots, y_n を所定のビット数だけある方向に回転し、そうでない場合、これとは逆の方向に回転するように構成することができる。

【0042】

本発明の他の観点に係るプログラムは、コンピュータを、上記の乱数列生成装置として機能させるように構成する。

【0043】

本発明の他の観点に係るプログラムは、コンピュータに、上記の乱数列生成方法を実行させるように構成する。

10

20

30

40

【0044】

これらのプログラムは、コンパクトディスク、フレキシブルディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、半導体メモリ等のコンピュータ読取可能な情報記録媒体に記録することができる。

【0045】

上記プログラムは、当該プログラムが実行されるコンピュータとは独立して、コンピュータ通信網を介して配布・販売することができる。また、上記情報記録媒体は、当該コンピュータとは独立して配布・販売することができる。

【0046】

【発明の実施の形態】

以下に本発明の実施形態を説明する。なお、以下に説明する実施形態は説明のためのものであり、本願発明の範囲を制限するものではない。したがって、当業者であればこれらの各要素もしくは全要素をこれと均等なものに置換した実施形態を採用することが可能であるが、これらの実施形態も本願発明の範囲に含まれる。

【0047】

(発明の実施の形態)

以下で説明する本発明の実施形態においては、「wビットの数値表現による乱数」の列を生成するために、有限体上の非線型変換として、所定の写像 $h(\cdot)$ と所定の整数 q ($0 \leq q \leq 2^w - 1$) とを用いて

$$g(a, b) = 2b^2 + h(a)b + q \pmod{2^w}$$

により定義される写像 $g(\cdot, \cdot)$ を用いる。

【0048】

写像 $h(\cdot)$ としては、恒等写像

$$h(a) = a$$

を用いることができる。

【0049】

また、所定のマスク値 MASK を利用することにより、与えられた値 a の数値表現の所定のビットをクリアする演算

$$h(a) = a \text{ and MASK}$$

や、所定のビットを反転する演算

$$h(a) = a \text{ xor MASK}$$

を採用してもよい。

【0050】

さらに、最下位の2ビットを値01に変換する演算

$$h(a) = (a \text{ and } (\text{not } 3)) \text{ or } 1$$

などを採用することができる。

【0051】

ここで、各演算子は値 a の数値表現（整数表現）に対するもので、and はビット積（ビットアンド）、xor はビット排他的和（ビットエクスクルーシブオア）、not はビット反転（ビットノット）、or はビット和（ビットオア）にそれぞれ相当するものである。

【0052】

したがって、これらの演算は、コンピュータにおいては桁上がりや桁下がりなどを取りたてて考慮せずに、wビットの整数演算として用意されているものをそのまま適用して実現することができる。

【0053】

またwの値は、当該コンピュータのCPU (Central Processing Unit) に用意されている機械語のビット幅、もしくは、これよりも小さい幅に対応させることが望ましい。

【0054】

10

20

30

40

50

現在のところ、世界最高速のブロック暗号技術といわれている R C 6 は、有限体上の非線型変換

$$f(x) = 2x^2 + x \pmod{2^w}$$

を用いることによって実現されており、これによって、ある種から生成される乱数列は、これとは異なる種から生成される乱数列とは常に異なるものであり（１対１性）、生成される乱数列の最長周期が $2^w - 1$ となっている。

【００５５】

本実施形態において採用される写像 $g(\cdot, \cdot)$ は、R C 6 における有限体上の非線型変換をさらに一般化したものであり、

$$h(a) = 1;$$

$$q = 0$$

とした $g(\cdot, \cdot)$ を採用した場合には、R C 6 と同等の乱数列の生成能力を有する。なお、本発明においては、上記の R C 6 同等の写像の以外の写像を選択できるため、さまざまなバリエーションの乱数を得ることができる。

【００５６】

また、これ以外の演算や値を選択した場合にも、良好な乱数列が得られることが、実験により実証されている。

【００５７】

図１は、本実施形態に係る乱数生成装置の概要構成を示す模式図である。図２は、本実施形態に係る乱数生成装置において実行させる処理の制御の流れを示すフローチャートである。以下、これらの図を参照して、本実施形態について、詳細に説明する。

【００５８】

乱数列生成装置１０１は、 w ビットの乱数の列を生成し、種受付部１０２と、初期化部１０３と、変換部１０４と、回転部１０５と、更新部１０６と、出力部１０７と、を備える。

【００５９】

まず、乱数列生成装置１０１の種受付部１０２は、 w ビットの整数の列 s_1, s_2, \dots, s_n を種として受け付ける（ステップ S 2 0 1）。

【００６０】

典型的には、 s_1, s_2, \dots, s_n は、乱数列生成装置が有する R A M (R a n d o m A c c e s s M e m o r y) 等のメモリに格納されるが、C P U が有するキャッシュに格納してもよいし、ハードディスク等の読み書き可能な外部記録媒体に一時的に記憶してもよい。

【００６１】

ついで、初期化部１０３は、当該受け付けられた s_1, s_2, \dots, s_n を、整数列 x_1, x_2, \dots, x_n として変換部１０４に与える（ステップ S 2 0 2）。

【００６２】

ここで、 x_1, x_2, \dots, x_n も同様に、R A M 等のメモリに格納される。この場合、初期化部１０３が実行する処理は、 s_1, s_2, \dots, s_n に対応するメモリから x_1, x_2, \dots, x_n に対応するメモリへの値の転送によって実現することができる。

【００６３】

さらに、変換部１０４は、当該与えられた整数列 x_1, x_2, \dots, x_n のそれぞれに対して上記の非線型変換 $g(\cdot, \cdot)$ により定義される変換を施して w ビットの整数の列 y_1, y_2, \dots, y_n を得る（ステップ S 2 0 3）。

【００６４】

当該変換としては以下のような漸化式により定義されるものを採用することができる。

【００６５】

(1) 整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_i = g(x_n, x_1);$$

$$y_{i+1} = g(x_1, x_{i+1})$$

10

20

30

40

50

により変換を行う。

【0066】

(2) 所定の整数 c を用いて、整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_i = g(c, x_i);$$

$$y_{i+1} = g(y_i, x_{i+1})$$

により変換を行う。

【0067】

(3) 整数 i ($1 \leq i \leq n-1$) についての漸化式

$$y_i = g(c, x_i);$$

$$y_{i+1} = g(x_i, x_{i+1})$$

により変換を行う。

【0068】

これらの計算は、CPUが有するALU (Arithmetic Logic Unit) を用いて実現することができる。 y_1, y_2, \dots, y_n もまた、メモリ等に格納される。

【0069】

そして、回転部105は、当該 y_1, y_2, \dots, y_n を wn ビットのビット列と見て所定の回転演算を行って、得られた wn ビットのビット列から w ビットの整数の列 z_1, z_2, \dots, z_n を得る(ステップS204)。

【0070】

所定の回転演算としては、以下のようなものを採用することができる。

【0071】

(1) wn ビットのビット列を所定のビット数だけ巡回シフトするもの。図3に、この巡回シフトとして、 $w=4, n=4$ であって、 y_1, y_2, \dots, y_4 をビッグエンディアンに配列して、1ビット左にシフトする場合の概要構成を示した。

【0072】

(2) 他の乱数をさらに取得して、これによって、回転方向および回転ビット数を決めるもの。たとえば、以下のような態様が考えられる。

(i) 得られた乱数が所定の値である場合ある方向に所定のビット数だけ回転し、そうでない場合、これとは逆の方向に所定のビット数だけ回転させる。たとえば、得られた乱数が奇数の場合は左に1ビット、偶数の場合は右に1ビット巡回シフトする。

(ii) 得られた乱数の値のビット数だけ左に巡回シフトする。

(iii) 得られた乱数の値を符号付整数と見て、その符号付整数の値だけ左に巡回シフトする(負の場合は、その絶対値分だけ右に巡回シフトすることになる)。

【0073】

これは、メモリ等に格納された y_1, y_2, \dots, y_n を、CPUにとって自然なビット幅単位で、桁上がり・桁下がり考慮しつつ、順次巡回シフトすることによって実現することができる。この場合、得られる z_1, z_2, \dots, z_n は、 y_1, y_2, \dots, y_n が格納されていたメモリ内の領域に新たな値として格納されることとなる。

【0074】

さらに、出力部107は、変換部104における変換ならびに回転部105における回転が、所定の回数繰り返されたか否かを判定する(ステップS206)。

【0075】

たとえば、ステップS201の前において、メモリ内に用意されたカウンタ変数に「所定の回数の値」を代入し、ステップS205とステップS206の間において当該カウンタ変数の値を1減じ、ステップS206においては、当該カウンタ変数の値が0になったか否かを判定することによって、実現することができる。

【0076】

所定の回数繰り返された場合(ステップS206; Yes)最後に得られた z_1, z_2, \dots, z_n を、乱数列 r_1, r_2, \dots, r_n として出力して(ステップS207)、乱数列

10

20

30

40

50

の生成を終了する。

【0077】

一方、所定の回数繰り返されていない場合（ステップS206；No）、更新部106は、当該 z_1, z_2, \dots, z_n を整数列 x_1, x_2, \dots, x_n として変換部104に与えて（ステップS205）、ステップS203に戻り、変換（ステップS203）、回転（ステップS204）の処理を繰り返す。

【0078】

これは、 z_1, z_2, \dots, z_n が格納されているメモリ等内の値を、 x_1, x_2, \dots, x_n が格納されているメモリ等へ転送することによって実現できる。

【0079】

乱数列生成装置101においては、図示しない記憶部が存在し、その記憶部は、 $s_1, s_2, \dots, s_n, x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n, z_1, z_2, \dots, z_n, r_1, r_2, \dots, r_n$ などを異なる領域に、もしくは、値の利用の依存関係を分析することにより、同じ領域に記憶する（たとえば、 y_1, y_2, \dots, y_n と z_1, z_2, \dots, z_n 等。）ような構成をとることができる。また、各部は、上記の共有メモリを用いて互いに計算した値をやりとりするのである。

【0080】

図4は、本実施形態の乱数列生成装置101が実現されるコンピュータの典型的な概要構成を示す模式図である。以下、本図を参照して説明する。

【0081】

コンピュータ301は、CPU 302によって制御される。コンピュータ301に電源が投入されると、CPU 302は、ROM（Read Only Memory）303に用意されたIPL（Initial Program Loader）を実行する。

【0082】

そして、IPLの実行により、フレキシブルディスクドライブ304に装着されたフレキシブルディスクやハードディスク305等に記録されたOS（Operating System）がロードされ、ユーザからの各種の指示入力を受け付けることができるようになる。

【0083】

ユーザは、キーボード306やマウス307を操作して、コンピュータ301に対して各種の指示入力を与える。

【0084】

これに応じて、OSは、ハードディスク305やCD-ROM（Compact Disk ROM）ドライブ308に装着されたCD-ROMに記録されたプログラムや各種のデータをCPU 302に実行させ、実行の過程やその結果をディスプレイ309に表示する。

【0085】

また、CPU 302は、一時的な記憶域として、RAM 311を利用する。RAM 311は、上記のように、計算の途中で利用される各種の数列を記憶するために用いられる。

【0086】

さらに、CPU 302は、プログラムの実行の過程において、ハードディスク305に、生成された乱数列などの処理の結果や途中経過などの情報を保存することができる。

【0087】

なお、本実施形態における演算は、上記のように、きわめて単純なビット演算に還元することができる。したがって、専用の電子回路（加算器、減算器、シフタ、ラッチ等）を組み合わせて乱数列生成装置101を構成することができるほか、DSP（Digital Signal Processor）やFPGA（Field Programmable Gate Array）などのような電子回路の構成状態を可変に変更できる電子素子を利用して、乱数列生成装置101を構成することができ、これらの態様も本発明の

10

20

30

40

50

範囲に含まれる。

【0088】

(実験の結果)

上記実施形態に係る乱数列生成装置101を用いて、以下の諸元で乱数列を生成させた。

$W = 32,$

$n = 32,$

$g(a, b) = 2b^2 + h(a)b$

【0089】

ただし、写像 $h(\cdot)$ は、与えられた値の数値表現の最下位2ビットを01に置換する演算により定義される。

10

【0090】

また、変換および回転は、それぞれ1ラウンドごとに1回とした。すなわち、「所定の回数の繰り返し」は1回である。

【0091】

出力されるのは、全部で $wn = 1024$ ビットの乱数列 $r_1, r_2, \dots, r_{1024}$ である。

【0092】

これに対して 20000×89999 種類の種を与え、 20000×89999 ラウンドだけ乱数列 $r_1, r_2, \dots, r_{1024}$ を出力させた。

【0093】

そして、これに対して乱数列のランダム性を検査する標準的なテストである FIPS 140-1 ならびに FIPS 140-2 のうち、標準セキュリティ規格にあるランダム性検査テストを、1024ビットの乱数列の中の各ビット位置毎に適用して、本実施形態の乱数列の性質を検査した。

20

【0094】

これらのテストにおいては、各ビット位置から20000ビットのビット列を取り出し、その20000ビットのビット列に対して、以下が行われる。

モノビットテスト (monobit test)。所定の位置のビットの値の出現頻度に偏りがないか否かを調べるもの。

ポーカータテスト (poker test)。20000ビットを5000個の4ビットパターンに分割し、その4ビットパターンの出現頻度に偏りがないか否かを調べるもの。

30

ランズテスト (runs test)。乱数列から所定の長さの連を切り出した場合に、当該長さの連の出現頻度に偏りがないか否かを調べるもの。長さとしては1~6を用いる。

ロングランズテスト (long runs test)。ランズテストと同様であるが、FIPS 140-1 の場合は34以上の連が存在する場合ランダム性が否定され、FIPS 140-1 の場合は26以上の連が存在する場合ランダム性が否定される。

【0095】

実験の結果、FIPS 140-1 においては、生成された1024ビット \times 89999 サンプルの20000ビット列は、すべて、定められた基準をクリアした。

40

【0096】

また、FIPS 140-2 においては、生成された1024ビット \times 89999 サンプルの20000ビット列の内、99.92パーセントのサンプルが、定められた基準をクリアした。

【0097】

また、本技術を XILINX (登録商標) 社の Vertex xcvt1000 (システムゲート数は100万) のFPGAに実装したところ、本アルゴリズムの並列性から、25.62Gビット/secのスピードで乱数列を生成させることができた。すなわち、本技術をFPGA等のハードウェアに実装すると、高速性の上で多大なメリットを得ることができる。

50

【0098】

このようにして、本実施形態によって生成された乱数列は極めて性質が良いものであり、秘密通信の暗号化の分野や物理現象、化学現象などの模擬実験の分野で有用であり、ハードウェア上で高速に良好なランダム性を持つ乱数列を出力するのに極めて有用であることが示された。

【0099】

【発明の効果】

以上説明したように、本発明によれば、生成される乱数列が乱数列として好ましい性質を有するような乱数列生成装置、乱数列生成方法、ならびに、これらをコンピュータによって実現するためのプログラムを提供することができる。

10

【図面の簡単な説明】

【図1】本発明の実施形態に係る乱数列生成装置の概要構成を示す模式図である。

【図2】本実施形態の乱数列生成装置において実行される乱数列生成処理の制御の流れを示すフローチャートである。

【図3】本実施形態の乱数列生成装置の回転部において実行される回転演算の様子を示す説明図である。

【図4】本実施形態の乱数列生成装置が実現される典型的なコンピュータの概要構成を示す模式図である。

【符号の説明】

101 乱数列生成装置

20

102 種受付部

103 初期化部

104 変換部

105 回転部

106 更新部

107 出力部

301 コンピュータ

302 CPU

303 ROM

304 フレキシブルディスクドライブ

30

305 ハードディスク

306 キーボード

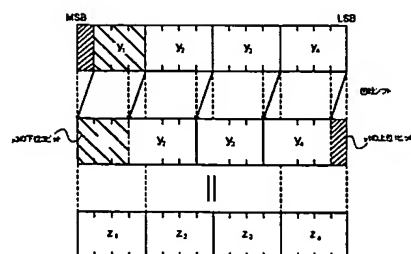
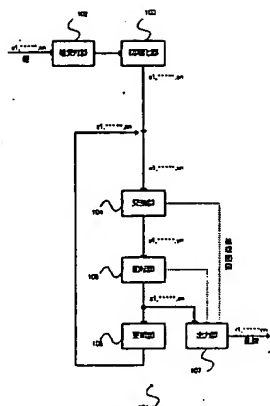
307 マウス

308 CD-ROMドライブ

309 ディスプレイ

311 RAM

【图 3】



【图 4】

